

ABSTRACT

A method is provided for communicating authenticated information concerning a digital public key certificate. A hash-tree data structure is created containing a pre-defined
5 list of possible information, such as authorizations, restrictions, privileges, or validity period notices. The list items may include text and coded values. Each list entry is prefixed with a different random data (blocker) value that is securely stored and infeasible to guess. Each list item is hashed to produce a leaf hash, the leaf hashes are combined to produce a hash tree, and the root node of said tree is embedded into a digital certificate or
10 message that is signed using a private key. In response to a request for authenticated information concerning a digital public key certificate, the certificate authority releases the relevant list item, its blocker value, and other hash values sufficient to authenticate the list item using the root node embedded in the digital certificate.